AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

Keonte BLOCKMON,

Defendant(s)

Case No. 8:23-mj-00400-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date of July 22, 2023 in the county of Orange in the Central District of California, the defendant violated:

Code Section	*Offense Description*
18 U.S.C. § 1951(a)	Interference with Commerce by Robbery

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

Complainant's signature

WYATT HACCOU, Special Agent, ATF
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 8/9/23

Judge's signature

City and state: Los Angeles, California

Hon. CHARLES F. EICK, U.S. Magistrate Judge
Printed name and title

AUSA: JMC X6520

AFFIDAVIT

I, Wyatt Haccou, being duly sworn, declare and state as follows:

1. I am a currently assigned to the ATF Los Angeles Field Division, Santa Ana Field Office, and have been employed by the ATF since December 2021. I have assisted in numerous investigations involving criminal street gangs, possession of firearms by prohibited persons, possession of stolen firearms, possession of machineguns, the illegal distribution of firearms, burglaries, robberies, carjackings, and other violent crimes. I have been involved with numerous serial robbery investigations involving a suspect or suspects committing multiple robberies, most of which were armed, of various businesses over a short period of time. Currently, I am assigned to the ATF Orange County Violent Crime Task Force (OCVCTF) based in Orange County, California. This Task Force is dedicated to identifying, tracking, and apprehending armed violent offenders committing criminal violations, to include but not limited to violations of Hobbs Act Robbery and other firearm related violations.

2. I received training during the course of my employment as an ATF Special Agent in various topics to include but not limited to: Robberies affecting interstate commerce, interview techniques, illegal trafficking of firearms, the utilization of informants, the activities of criminal street gangs, asset forfeiture, and conducting surveillance and wire interceptions. Through these investigations, my training and experience, and conversations with other experienced agents and law enforcement

personnel, I have become familiar with the methods used by individuals to plan and commit robberies, to acquire, smuggle, safeguard, store firearms, and to distribute firearms. I am also familiar with how controlled substances are imported, manufactured, distributed, and sold. I have become familiar with the schemes of the individuals engaged in the illegal importation, smuggling, manufacturing, and sales of firearms and controlled substances.

3. In the course of the cases I investigate, I routinely use cellular technology and records, such as cell phone location information, cell site simulators, and call detail records to obtain evidence of conspiracies to commit robberies, burglaries, carjackings, and the trafficking of firearms and controlled substances.

I. PURPOSE OF THE AFFIDAVIT

4. This affidavit is made in support of the following:

a. A criminal complaint charging Keonte BLOCKMON ("BLOCKMON") with violation of 18 U.S.C. § 1951(a), conspiracy to interfere with commerce and interference with commerce by robbery and;

b. An application for search warrants to search the following digital devices (identified below as SUBJECT DEVICES 1, 2, and 3), in custody of the Irvine Police Department, in Irvine, California:

i. An Apple iPhone 14 Pro Max with blue phone case booked into Irvine Police Department evidence under

property tag number 14207, seized from BLOCKMON on July 22, 2023. ("SUBJECT DEVICE 1");

ii. A white Apple iPhone with a brown case booked into Irvine Police Department evidence under property tag # 14209, seized from CC-1[1] on July 22, 2023 ("SUBJECT DEVICE 2"); and

iii. A space gray Apple iPhone with no case, booked into Irvine Police Department evidence under property tag #14208, seized from CC-2[2] on July 22, 2023 ("SUBJECT DEVICE 3").

5. The requested search warrants seek authorization to seize data on the SUBJECT DEVICES that constitute evidence or fruits in violation of 18 U.S.C. § 1951(a), conspiracy to interfere with commerce and interference with commerce by robbery, (the "Subject Offenses"). They also request to seize the SUBJECT DEVICES if they are themselves or they contain evidence, contraband, fruits, or instrumentalities of the Subject Offense, and forensic copies thereof.

6. The SUBJECT DEVICES are identified in Attachments A-1, A-2, and A-3 to the search warrant application. The list of items to be seized is set forth in Attachment B to the search warrant application. Attachments A-1, A-2, A-3, and B are incorporated herein by reference.

7. The facts set forth in this affidavit are based upon my observations, my training and experience, and information

---

[1] CC-1 was identified by law enforcement as a 17-year-old male from Los Angeles, California.

[2] CC-2 was identified by law enforcement as a 17-year-old male from Los Angeles, California

obtained from other law enforcement agents, officers, and investigators, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not purport to set forth all my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. SUMMARY OF PROBABLE CAUSE

8. On July 22, 2023, Irvine Police Department ("IPD") officers responded to a call at the Irvine Spectrum Mall located at 670 Spectrum Center Dr., Irvine, California 92618 regarding a robbery that occurred at a Kay Jewelers store. The total loss amount was approximately $55,829.66. Shortly after the robbery, IPD officers located the gray Honda Sedan suspect vehicle and conducted a felony car stop. Subsequently, IPD officers arrested BLOCKMON and recovered the SUBJECT DEVICES. BLOCKMON and the SUBJECT DEVICES recovered were transported into IPD custody.

III. STATEMENT OF PROBABLE CAUSE

9. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. KAY JEWELERS ROBBERY - July 22, 2023

10. On July 22, 2023, at approximately 5:04 p.m., Irvine Spectrum Mall Security received a call regarding three suspicious subjects last seen in the area of the Nordstrom

parking structure. Around the same time, IPD dispatch received information that a robbery had just occurred at the Kay Jewelers store[3] at the Spectrum mall committed by three male suspects.

11. Surveillance video footage captured the suspects entering the Kay Jeweler store and showed three male suspects with slim builds, wearing dark colored hoodies, and covid style face masks. The three suspects entered the store and immediately began smashing the glass display cases with hammers and subsequently began grabbing various amounts of jewelry out of the shattered display cases. The three suspects left the store on foot toward an unknown direction. IPD officers contacted a Kay Jeweler customer that was inside the store during the robbery who stated he was in fear for his life during the robbery.

12. As IPD dispatch was receiving additional information from the aforementioned robbery, the mall security received a call regarding a hit-and-run collision that occurred in the area of the Nordstrom parking structure of the Irvine Spectrum mall. The hit-and-run collision occurred in the same area where the original call was broadcast regarding the three suspicious subjects. The three suspicious subjects matched the description of the suspects who committed the robbery inside the Kay Jewelers store. IPD officers responded to the collision and

[3] Kay Jewelers is part of a collection of companies owned and operated by Signet Jewelers, an international diamond retailer headquartered in Ohio engaged in domestic and foreign commerce. Signet Jewelers is a publicly traded company and operates approximately 2,800 stores worldwide.

obtained a photo from the witness of a gray/silver Honda sedan, with front bumper damage, a black rear bumper, and bearing California license plate 8AVA984.

B. FELONY STOP OF HONDA SEDAN WITH LICENSE PLATE 8AVA984

13. The description of the suspect vehicle and the license plate 8AVA984 was broadcast to IPD patrol officers in the nearby area. An IPD Officer observed the suspect vehicle on the I-5 freeway traveling northbound past the Sand Canyon exit. The IPD Officer advised IPD patrol units in the nearby area of the vehicle and its direction while remaining behind the suspect vehicle without any emergency lights or sirens activated. Additional IPD units responded and initiated a felony car stop on the I-5 northbound freeway near Jamboree Road. The suspect vehicle then pulled over.

14. The three suspects were removed from the vehicle and detained by IPD officers. The suspects were identified as CC-1 (Driver), CC-2 (Front Passenger), and Keonte BLOCKMON (rear passenger). Inside the vehicle, in plain view, were masks and hammers that were seen being used during the Kay Jewelers robbery. Additionally, IPD Officer Vespia further searched the vehicle and noticed a multicolored backpack sitting on the rear driver side seat. The backpack was open and in plain view were large amounts of jewelry items, multiple display stands, and numerous pieces of broken glass, consistent with the items taken during the robbery. Furthermore, Officer Vespia noticed that the jewelry items contained price tags on them. Officer Vespia transported the jewelry and other miscellaneous items found

inside the backpack to the Kay Jewelers store and confirmed with store employees that the jewelry found in the backpack belonged to the business and was stolen.

C. SUSPECT CLOTHING

15. All three suspects were found to be wearing clothing consistent with the robbery suspects:

a. CC-1 was wearing a black and grey hooded jacket with "Nike Air" in white letting across the chest. Underneath the hooded jacket was a plain navy-blue t-shirt. CC-1 was wearing black Adidas sweatpants and black "Nike" branded shoes. CC-1 was wearing similar clothing during the robbery.

b. CC-2 was wearing a black hooded jacket with "Nike Air" in white letting across the chest. Underneath the jacket, CC-2 was wearing a white tank top, black sweatpants that had "Hollister California" written on the left pant leg, and multicolored socks with white "Nike" branded shoes. CC-2 was wearing similar clothing during the robbery.

c. Lastly, BLOCKMON was wearing a white tank top, black sweatpants, white and blue Nike Air Jordan shoes, and a black Nike sweatshirt hoodie. BLOCKMON was wearing similar clothing during the robbery.

D. BLOCKMON INTERVIEW

16. BLOCKMON was advised of his Miranda rights, and agreed to speak to IPD officers. During the interview, BLOCKMON admitted to committing the robbery. Specifically, IPD officers showed BLOCKMON surveillance footage of the robbery and pointed to the suspect holding the Kay Jewelers' front door open,

allowing easier access for the two additional suspects to commit the robbery. IPD officers asked BLOCKMON if that was him holding the door, to which BLOCKMON said it was. BLOCKMON also admitted to being in the car during the hit-and-run collision that occurred in the area of the Nordstrom parking lot. Lastly, BLOCKMON told IPD officers that after the robbery, while fleeing in the suspect vehicle, he reached inside the multicolored backpack and started grabbing gold chains and other jewelry items consistent with what IPD found after the car stop.

E. BLOCKMON CRIMINAL HISTORY

17. Based on my review of BLOCKMON's criminal history, I learned that BLOCKMON has prior arrests for firearms offenses dating back to 2020.

IV. TRAINING AND EXPERIENCE ON ROBBERY OFFENSES

18. From my training, personal experience, and the collective experiences related to me by other law enforcement officers who conduct robbery investigations, I am aware of the following:

a. Persons who engage, participate, or are involved with robberies generally maintain records of their stolen merchandise items and usually keep them in their residence, or in places that are readily accessible, and under their physical control, such as in their digital devices. It has been my experience that people who participate in robberies will keep the contact information of other co-conspirators or other individuals involved in criminal activities for future purchases or referrals. Such information is also kept on digital devices.

b. Individuals involved in robberies frequently use their cell phones to coordinate with co-conspirators and to research robbery locations. Cell phones, for example, may be used to set meeting locations, pick routes to the robberies, coordinate times, and recruit robbery crew members.

c. Many people also keep mementos from their robberies, including digital photographs or recordings of themselves possessing stolen merchandise items from the respected business from which the robbery occurred at. These photographs and recordings are often shared via social media, text messages, and over text message applications.

d. Those who commit robberies often sell the stolen merchandise or keep in their possession. Correspondence between persons buying and selling stolen merchandise often occurs over phone calls, e-mail, text message, and social media message to and from smartphones, laptops, or other digital devices. This includes sending photographs of the stolen merchandise between the seller and the buyer, as well as negotiation of prices. In my experience, people who engage in sales of stolen property frequently use phone calls, e-mail, and text messages to communicate with each other regarding stolen merchandise that they sell or offer for sale. In addition, it is common for individuals who engage in robberies to have photographs of the stolen merchandise they or other individuals working with them possess or their cellular phones and other digital devises as they frequently send these photos to each other to boast of

their stolen merchandise and/or to facilitate sales or transfers of the stolen merchandise.

e. Individuals who engage themselves in robberies often use multiple digital devices to minimize the chance of being traced. Additionally, multiple digital devices are often used for communicating with lookout vehicles and other co-conspirators who engage themselves in committing robberies.

V. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

19. As used herein, the term "digital device" includes the SUBJECT DEVICES.

20. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

b. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

c. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of

evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

d. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

e. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

21. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I

know that it can take a substantial period of time to search a digital device for many reasons, including the following:

f. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above.

g. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

22. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

h. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition

function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

i. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the SUBJECT DEVICES.

j. The person who is in possession of a device or has the device among his or her belongings is likely a user of the device. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress CC-1, CC-2, and BLOCKMON'S thumb(s)- and/or fingers on the device(s); and (2) hold the device(s) in front of CC-1, CC-2, and BLOCKMON'S face with their eyes open to activate the facial-, iris-, and/or retina-recognition feature.

k. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VI. CONCLUSION

23. For the reasons described above, there is probable cause to believe that BLOCKMON has committed a violation of Title 18, United States Code, Section 1951(a), conspiracy to interfere with commerce and interference with commerce by

robbery. Similarly, for the reasons described above, there is probable cause to believe that the items listed in attachment B, which constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1951(a), will be found on the SUBJECT DEVICES, as described in Attachments A-1, A-2, and A-3.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 9th day of April 2021.

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

DEVICE TO BE SEARCHED

a. 1. An Apple iPhone 14 Pro Max with blue phone case booked into Irvine Police Department evidence under property tag number 14207, seized from Keonte BLOCKMON on July 22, 2023. ("SUBJECT Device 1")

ATTACHMENT A-2

DEVICE TO BE SEARCHED

a. A white Apple iPhone with a brown case booked into Irvine Police Department evidence under property tag # 14209, seized from CC-1 on July 22, 2023. ("Subject Device 2").

ATTACHMENT A-3

DEVICE TO BE SEARCHED

b. A space gray Apple iPhone with no case, booked into Irvine Police Department evidence under property tag #14208, seized from CC-2 on July 22, 2023. ("SUBJECT DEVICE 3")

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violation of 18 U.S.C. § 1951(a), conspiracy to interfere with commerce and interference with commerce by robbery (the Subject Offense), namely:

a. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from the SUBJECT DEVICES, all received or missed incoming calls, and all telephone numbers accessed through any push-to-talk functions;

b. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show text messages, email communications, or other text or written communications sent to or received from the SUBJECT DEVICES and which relate to the Subject Offense;

c. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), text messages, email communications, or other text or written communications sent to or received from the SUBJECT DEVICES and which relate to the Subject Offense;

d. Records, documents, programs, applications, materials, or conversations relating to the above-named violations, including correspondence, receipts, records, and documents noting prices or times when guns or ammunition were bought, sold, or otherwise distributed;

e. Audio or video recordings, or images relating to the Subject Offense, or relating to the collection or transfer of proceeds of the Subject Offense;

f. Audio or video recordings, images, records, documentation, or instructions relating to the purchase, sale, or robbery components;

g. Contents of any calendar or date book;

h. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

i. A SUBJECT DEVICE if it is itself or contains evidence, contraband, fruits, or instrumentalities of the Subject Offense, and forensic copies thereof.

j. With respect to the SUBJECT DEVICES containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created,

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

II. SEARCH PROCEDURE FOR THE SUBJECT DEVICES

3. In searching the SUBJECT DEVICES (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any SUBJECT DEVICE capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search the SUBJECT DEVICES where they are currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the SUBJECT DEVICES as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the digital devices beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each SUBJECT DEVICE capable of containing any of the items to be seized to the search protocols to determine whether the SUBJECT DEVICES and any data thereon falls within

the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

f. If the search determines that a SUBJECT DEVICE does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return that SUBJECT DEVICE and delete or destroy all forensic copies thereof.

g. If the search determines that a SUBJECT DEVICE does contain data falling within the list of items to be seized, the government may make and retain copies of such data and may access such data at any time.

h. If the search determines that a SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling

within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain the SUBJECT DEVICE if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the SUBJECT DEVICE, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

4. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

5. During the execution of this search warrant, law enforcement is permitted to (1) depress CC-1, CC-2, and

BLOCKMON'S thumb(s)- and/or fingers onto the fingerprint sensor of the SUBJECT DEVICES (only if the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of CC-1, CC-2, and BLOCKMON'S face(s) with their eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.